

**CROSS-BORDER PRIVACY RULES SYSTEM JOINT OVERSIGHT
PANEL**

**ADDENDUM TO THE RECOMMENDATION REPORT ON APEC
RECOGNITION OF TRUST^e**

Submitted To: Ms. Lourdes Yaptinchay

Chair, APEC Electronic Commerce Steering Group

12 April 2013

TABLE OF CONTENTS

Executive Summary.....	1
Business Proprietary Information.....	2
Applicability of CBPR Certification to Offline Data Privacy Practices	2
Jurisdiction.....	3
Conflicts of Interest.....	3
Program Requirements.....	5
Certification Process.....	5
Ongoing Monitoring and Compliance Review	6
Recertification.....	7
Dispute Resolution.....	8
Mechanism for Enforcing Program Requirements.....	9
Case Notes and Statistics.....	9
Annex A.....	11

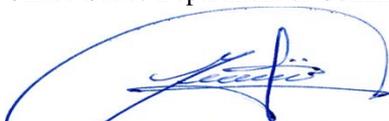
EXECUTIVE SUMMARY

On 20 February 2013, the Cross Border Privacy Rules (CBPR) system's Joint Oversight Panel¹ (JOP) circulated its recommendation report to APEC member Economies regarding TRUSTe's application for APEC recognition to participate as an Accountability Agent in the United States as part of the CBPR system. In that report, the JOP concluded that in its opinion, TRUSTe had met each of the Recognition Criteria as identified in the APEC Accountability Agent Recognition Application. APEC member Economies were then asked to make a determination as to TRUSTe's request for recognition, taking into account the JOP's recommendation. To facilitate this deliberative process, paragraph 20 of the *Protocols of the APEC Cross-Border Privacy Rules System Joint Oversight Panel* states that "[a]ny APEC member Economy may request additional information or clarification from the applicant Accountability Agent when making a determination on whether to grant the applicant Accountability Agent's request for recognition." Pursuant to this, Australia has asked for clarification on a number of issues in the JOP Recommendation Report after having undertaken domestic consultations. These issues were circulated to APEC member Economies by the Data Privacy Subgroup Chair on 19 March 2013. Following is additional information for Member Economy consideration regarding the issues circulated by Australia (hereafter "comments") as they pertain to identified recognition criteria.

Signed,



Josh Harris
Chair, Joint Oversight Panel
United States Department of Commerce



Elizabeth Argüello Maya
Co-Chair, Joint Oversight Panel
Ministry of Economy, Mexico



Susan Lu
Co-Chair, Joint Oversight Panel
Bureau of Foreign Trade, Chinese Taipei

12 April 2013

¹ For purposes of this addendum, JOP membership consist of: Josh Harris, United States Department of Commerce; Elizabeth Argüello Maya, Ministry of Economy, Mexico; and Susan Lu, Bureau of Foreign Trade, Chinese Taipei

Business Proprietary Information

In the circulated comments, it was suggested that business proprietary designation be used only under exceptional circumstances. Paragraph 20 of the *Protocols of the APEC Cross-Border Privacy Rules System Joint Oversight Panel* states “[t]he recommendation report will not contain any business proprietary or confidential information of the applicant Accountability Agent.” For purposes of the consultative process between the JOP and the applicant Accountability Agent, the designation of any document or information as “proprietary” is assigned by the applicant Accountability Agent and can be afforded to any information an applicant Accountability Agent otherwise keeps confidential. However, the JOP recognizes the importance of facilitating a Member Economy’s thorough assessment of any Accountability Agent application. To accommodate both interests, the JOP stated in footnote 13 of its Recommendation Report that when a Member Economy has further questions regarding any business proprietary documentation referenced, that Economy should contact the JOP directly for direct review and further discussion as necessary. The intent of this provision is to facilitate the consultative process in a way that protects the confidentiality of any proprietary information while ensuring a Member Economy has the information necessary to make a determination as to the sufficiency of the applicant Accountability Agent’s fulfillment of the associated recognition criteria.

Applicability of CBPR Certification to Offline Data Privacy Practices

The comments question the applicability of TRUSTe’s seal to offline collection practices. Question 1 in the *CBPR Intake Questionnaire* asks a company seeking CBPR certification “Do you provide clear and easily accessible statements about your practices and policies that govern the personal information described above (a privacy statement)? Where YES, provide a copy of all applicable privacy statements and/or hyperlinks to the same.” In the corresponding assessment criteria, the Accountability Agent must verify that the company’s “privacy practices and policy include the following characteristics:…Applies to all personal information; whether collected online or offline.” In its consultations with TRUSTe, the JOP confirmed that for purposes of CBPR certification, TRUSTe will not distinguish between online and offline collected data in its program requirements. As such, the requirements of the CBPR system extend to any medium through which a company seeking CBPR certification collects personal data. This finding is noted in question 1, column 3 of Annex C to the JOP Recommendation Report.

In addition, TRUSTe has since confirmed that it intends to offer a unique seal that indicates CBPR certification, although this is not a requirement for APEC recognition and is at the discretion of each applicant Accountability Agent.

Paragraph 21 of the *Protocols of the APEC CBPR Joint Oversight Panel* stipulates that “[o]nce recognized, Accountability Agents must make their completed *APEC Accountability Agent Recognition Application* (excluding all business proprietary or confidential information) available on their website and easily accessible to consumers.” As part of its

consultation process, the JOP confirmed that TRUSTe will post all CBPR-certified companies online as well as the applicable CBPR program requirements on its website. This finding is noted in Section I of the Recommendation Report (*Enforceability*).

The JOP also consulted with the United States Federal Trade Commission (FTC) on the enforceability of each program requirement, including the provision identified above. The FTC confirmed that a company certified by an Accountability Agent under the CBPR system must publicly declare that it will comply with all CBPR program requirements and must make these program requirements publicly accessible. If the company fails to comply with any of these program requirements, its public representation of compliance may constitute an unfair or deceptive act or practice subject to enforcement pursuant to Section 5 of the FTC Act, 15 U.S.C. § 45².

Jurisdiction

The comments also requested clarification as to the jurisdiction of the FTC. The JOP has confirmed with the FTC that TRUSTe is subject to FTC jurisdiction, regardless of any jurisdiction states may also have under state law, and regardless of incorporation in one state with headquarters in another. The Federal Trade Commission's legal authority is found in Section 5 of the Federal Trade Commission Act ("FTC Act"), which prohibits "unfair or deceptive acts or practices" in or affecting commerce. 15 U.S.C. § 45. "Commerce" is defined in the FTC Act as including "commerce among the several States or with foreign nations." 15 U.S.C. § 44. Pursuant to the FTC Act, the Federal Trade Commission has jurisdiction over corporations and other entities. 15 U.S.C. § 45(a)(2). TRUSTe is a for-profit corporation that engages in commerce across states. Although certain types of entities and activities are excluded from FTC enforcement authority under the Federal Trade Commission Act, see 15 U.S.C. 45(a)(2), it does not appear that TRUSTe engages in any activities that would preclude or limit FTC jurisdiction.

Conflicts of Interest

Clarification was requested as to how "TRUSTe would deal with the situation of applications for certification from businesses which have a commercial interest in TRUSTe (or of complaints about such businesses if certified)." This request for clarification specifically relates to Accountability Agent Recognition Criterion 2(a) and (b), which states in part that "[a]t no time may an Accountability Agent have a direct or indirect affiliation with any Applicant organization or Participant organization that would prejudice the ability of the Accountability agent to render a fair decision with respect to their certification and ongoing participation in the CBPR System..."

² The FTC enforces Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits unfair or deceptive acts or practices in or affecting commerce. An act or practice is deceptive if it is likely to mislead a consumer acting reasonably under the circumstances and is likely to affect a consumer's conduct or decision regarding a product or service.

As noted in the Recommendation Report, TRUSTe is required under law to apply its certification standards in an impartial manner, pursuant to Title 15, Chapter 22, Subchapter I, § 1064 of the United States Code. In addition, TRUSTe's Articles of Incorporation imposes penalties on any member of the Board of Directors who violates their duty of loyalty to TRUSTe, which includes any knowing violation of this or any other law. *See TRUSTe Articles of Incorporation Art. 9 ("A director of this corporation shall not be personally liable to this corporation or its stockholders for monetary damages for breach of fiduciary duty as a director, except for liability (i) for any breach of the director's duty of loyalty to this corporation or its stockholders, (ii) for acts or omissions not in good faith or that involve intentional misconduct or a knowing violation of law, (iii) under Section 174 of the General Corporation Law³, or (iv) for any transaction from which the director derived any improper personal benefit").* The Joint Oversight Panel is satisfied that these requirements satisfy the prohibition established in Accountability Agent Recognition Criterion 2(a).

Accountability Agent Recognition Criterion 2(b) lists the types of affiliations that "may be cured by the existence of structural safeguards or other procedures undertaken by the Accountability Agent" and requires their prompt disclosure to the JOP, along with an explanation of the "safeguards in place to ensure that such affiliations do not compromise the Accountability Agent's ability to render a fair decision with respect to such an Applicant organization or Participant organization." As stated in the Recommendation Report, TRUSTe has agreed to provide such information to the JOP in the event that such an identified situation arises.

This Recognition Criterion further requires TRUSTe to submit an overview of its "internal structural and procedural safeguards to address any of the potential or actual conflicts of interest identified in 2(b) of Annex A." In fulfillment of this requirement, TRUSTe submitted its Certification Conflicts of Interest Policy and detailed information on the separation of staff (designated as proprietary) for review by the Joint Oversight Panel to guard against conflicts of interest between the reviewer of a CBPR Participant and the reviewer's duty to neutrally apply the TRUSTe privacy program requirements.

Clarification was also requested as to the separation of TRUSTe's consulting and certification services. Recognition Criterion 2(d) permits an Accountability Agent to "perform consulting or technical services for an Applicant organization or Participant organization other than services relating to their certification and on-going participation in the CBPR System" and requires the Accountability Agent to disclose to the Joint Oversight Panel the existence of the engagement; and an explanation of the safeguards in place to ensure that the Accountability Agent remains free of actual or potential conflicts of interest arising from the engagement. As stated in the Recommendation Report, TRUSTe has stipulated that it will not engage with Participants it certifies to perform consulting services outside of those functions described in paragraphs 5 - 14 of the *Accountability Agent Recognition Criteria*.

³ Available at <http://delcode.delaware.gov/title8/c001/sc05/index.shtml#174>

Where TRUSTe does consult with regard to privacy practices not specifically addressed by a certification program, TRUSTe has stated that such work is executed by a member of the Legal department staff, as opposed to Operations staff. In addition to organizational separation of personal, TRUSTe provided the JOP with its Service Delivery Conflicts of Interest Policy (designated business proprietary). TRUSTe has informed the JOP that it engages in less than 20 such consulting engagements per year. As stated in the Recommendation Report, the JOP is satisfied that this information meets Accountability Agent Recognition Criterion 2(a), (b) and (d).

It was suggested that the JOP should require all conflict of interest policies to be made publically available. As discussed previously, an applicant Accountability Agent can designate as “proprietary” any document or information the applicant otherwise keeps confidential. The JOP stated in footnote 13 of its Recommendation Report that when a Member Economy has further questions regarding any business proprietary documentation referenced, that Economy should contact the JOP directly for direct review and further discussion. Should Member Economies wish to require that the conflicts of interest policies of an Accountability Agent applicant be made public, they may expressly incorporate such requirement into the Accountability Agent Recognition Criteria, pursuant to the established endorsement process (the consensus determination of Member Economies).

It was further suggested that TRUSTe’s conflicts of interest policies be endorsed by its Board of Directors. This is currently not a requirement under the endorsed Recognition Criteria. Should Member Economies determine that such endorsement should be required, they may expressly incorporate such a requirement into the Accountability Agent Recognition Criteria, pursuant to the established endorsement process (the consensus determination of Member Economies).

Program Requirements

As indicated in its Recommendation Report, the JOP worked in consultation with TRUSTe to map its program requirements to the CBPR system. The results of this consultation are found in Annex C to the Recommendation Report. Based on this consultation, the JOP concluded that each of the 50 CBPR program requirements had been successfully mapped against TRUSTe’s program requirements. This finding is noted in the JOP Recommendation Report under Section 4 (*Program Requirements*). Please see Annex A for additional discussion of questions associated with specific program requirements.

Certification Process

The comments suggested that the JOP should also consider reviewing the fee structure associated with an Accountability Agent’s certification process. As drafted, Accountability Agent Recognition Criterion 5 requires:

“An Accountability Agent has a comprehensive process to review an Applicant organization’s policies and practices with respect to the Applicant organization’s participation in the Cross

Border Privacy Rules System and to verify its compliance with the Accountability Agent’s program requirements. The certification process includes:

- a) An initial assessment of compliance, which will include verifying the contents of the self-assessment forms completed by the Applicant organization against the program requirements for Accountability Agents, and which may also include in-person or phone interviews, inspection of the personal data system, Web site scans, or automated security tools.
- b) A comprehensive report to the Applicant organization outlining the Accountability Agent’s findings regarding the Applicant organization’s level of compliance with the program requirements. Where non-fulfillment of any of the program requirements is found, the report must include a list of changes the Applicant organization needs to complete for purposes of obtaining certification for participation in the CBPR System.
- c) Verification that any changes required under subsection (b) have been properly completed by the Applicant organization.
- d) Certification that the Applicant organization is in compliance with the Accountability Agent’s program requirements. An Applicant organization that has received such a certification will be referred to herein as a “Participant” in the CBPR System.”

In addition to the explanation of the certification process provided in its recommendation report, the JOP consulted with TRUSTe to determine that each step of its certification process meets the listed recognition criteria, above. As part of this consultation, the JOP reviewed TRUSTe’s *Client Interview Form* and a sample *Findings Report* (business proprietary).

A review of the applicant Accountability Agent’s fee structure was not part of the JOP’s consultation since it falls outside of the scope of the endorsed recognition criteria. Under the current application process, there are no endorsed metrics against which the JOP can measure an applicant Accountability Agent’s fee structure. Should Member Economies determine that such a review should be undertaken as part of this consultation process, it must be expressly incorporated into the Accountability Agent Recognition Criteria, pursuant to the established endorsement process (the consensus determination of Member Economies).

Ongoing Monitoring and Compliance Review processes

The comments also questioned the applicability of TRUSTe’s ongoing monitoring and compliance and review process to offline activities. As noted above, the JOP confirmed that for purposes of CBPR certification, TRUSTe will not distinguish between online and offline collected data in its program requirements. As such, the requirements of the CBPR system, including those related to ongoing monitoring, extend to any medium through which a company seeking CBPR certification collects personal data. This finding is noted in question1, column 3 of Annex C to the JOP Recommendation Report.

Accountability Agent Recognition Criterion 6 requires that the “Accountability Agent has comprehensive written procedures designed to ensure the integrity of the Certification process and to monitor the Participant throughout the certification period to ensure compliance with the Accountability Agent’s program.” Accountability Agent Recognition Criterion 7 further requires that “where there are reasonable grounds for the Accountability

Agent to believe that a Participant has engaged in a practice that may constitute a breach of the program requirements, an immediate review process will be triggered whereby verification of compliance will be carried out...”).

In addition to the automated tools used to ensure compliance, TRUSTe stipulated in their application that “[a]dditional verification activities, including third-party onsite audits, may be warranted in certain circumstances both during certification and compliance.” TRUSTe further stated that each of these verification activities may be initiated by “an internal compliance investigation based on results of the technological monitoring, described above, or on information contained in a consumer complaint, news or press reports, regulator inquiry, or reports from other credible sources.” The JOP is satisfied that the combination of both automated and onsite verification activities, and the listed means of triggering these review mechanisms meet the requirements of Accountability Agent Recognition Criteria 6 and 7.

Recertification

The comments suggested that the JOP should further consider reviewing the fee structure associated with the recertification process. As drafted, Accountability Agent Recognition Criterion 8 states that:

“Accountability Agent will require Participants to attest on an annual basis to the continuing adherence to the CBPR program requirements. Regular comprehensive reviews will be carried out to ensure the integrity of the re-Certification. Where there has been a material change to the Participant’s privacy policy (as reasonably determined by the Accountability Agent in good faith), an immediate review process will be carried out. This re-certification review process includes:

- a) An assessment of compliance, which will include verification of the contents of the self-assessment forms (Project 1) updated by the Participant, and which may also include in-person or phone interviews, inspection of the personal data system, Web site scans, or automated security tools.
- b) A report to the Participant outlining the Accountability Agent’s findings regarding the Participant’s level of compliance with the program requirements.
- c) The report must also list any corrections the Participant needs to make to correct areas of non-compliance and the timeframe within which the corrections must be completed for purposes of obtaining re-certification.
- d) Verification that required changes have been properly completed by Participant.
- e) Notice to the Participant that the Participant is in compliance with the Accountability Agent’s program requirements and has been re-certified.”

As noted in the Recommendation Report, the JOP has confirmed that TRUSTe requires an annual re-certification at which time TRUSTe investigates whether the Participant is meeting and/or exceeding TRUSTe's Program Requirements.

A review of the applicant Accountability Agent's fee structure was not part of the JOP's consultation since it falls outside of the scope of the endorsed recognition criteria. As discussed previously, there are no endorsed metrics against which the JOP can measure an applicant Accountability Agent's fee structure. Again, should Member Economies determine that such a review must be undertaken pursuant to the consultation, it should be expressly incorporated into the Accountability Agent Recognition Criteria, pursuant to the established endorsement process (the consensus determination of Member Economies).

Dispute Resolution

It was also questioned whether TRUSTe meets Accountability Agent Recognition Criterion 13, which requires that an "Accountability Agent has processes in place to impose the following penalties, which is proportional to the harm or potential harm resulting from the violation, in cases where a Participant has not complied with the program requirements and has failed to remedy the non-compliance within a specified time period....

- a) Requiring Participant to remedy the non-compliance within a specified time period, failing which the Accountability Agent shall remove the Participant from its program.
- b) Temporarily suspending the Participant's right to display the Accountability Agent's seal.
- c) Naming the Participant and publicizing the non-compliance.
- d) Referring the violation to the relevant public authority or privacy enforcement authority. [*NOTE*: this should be reserved for circumstances where a violation raises to the level of a violation of applicable law.]
- e) Other penalties – including monetary penalties – as deemed appropriate by the Accountability Agent."

In its Recommendation Report, the JOP stated that it was satisfied that the process described by TRUSTe to suspend a participant if it does not remedy non-compliance within a specific time period (*Privacy Certification Program Requirements*, section III.5.a (1)-(5)) met Recognition Criteria 11-15, including Criterion 13, above. In making this recommendation, the JOP assessed TRUSTe's application against Criterion 13(a)-(d). While TRUSTe does not have authority by contract to impose monetary penalties (13(e)), this is not a requirement for recognition, but illustrative of additional penalties that an Accountability Agent may impose at its discretion.

The comments also noted that there is no reference to complainants being notified of their right to complain to a Privacy Enforcement Authority if they are dissatisfied with the

outcome of TRUSTe's dispute resolution process. It was correctly noted that this is not currently a Recognition Criterion. However, any person may directly contact the relevant Privacy Enforcement Authority in their Economy regarding the conduct of a CBPR-certified company. To date, recognition of this "no wrong door" approach has been considered part of the education and outreach activities of the Enforcement Authorities and Member Economies and is not an endorsed Recognition Criterion. Should Member Economies determine that such a criterion be established as a condition for APEC recognition, it should be expressly incorporated into the Accountability Agent Recognition Criteria, pursuant to the established endorsement process (the consensus determination of Member Economies).

Mechanism for Enforcing Program Requirements

The comments question whether TRUSTe meets Accountability Agent Recognition Criterion 14, which requires an applicant Accountability Agent to "refer a matter to the appropriate public authority or enforcement agency for review and possible law enforcement action, where the Accountability Agent has a reasonable belief pursuant to its established review process that a Participant's failure to comply with the APEC Cross-Border Privacy Rules System requirements has not been remedied within a reasonable time under the procedures established by the Accountability Agent pursuant to paragraph 2 so long as such failure to comply can be reasonably believed to be a violation of applicable law." As stated in the Recommendation Report, the JOP is satisfied that the procedures culminating in termination and referral described by TRUSTe in its application meet the express elements outlined above, including the ability of a participant to remedy within a reasonable time.

It was also questioned whether TRUSTe meets Accountability Agent Recognition Criterion 15, which states that "[w]here possible, Accountability Agent will respond to requests from enforcement entities in APEC Economies that reasonably relate to that Economy and to the CBPR-related activities of the Accountability Agent." This formulation is drawn from Paragraph 18 of the *APEC Cross Border Privacy Rules Policies, Rules and Guidelines*, which states that "an Accountability Agent should consent to respond to requests from relevant government entities in any APEC Economy that reasonably relate both to that Economy and to the CBPR-related work of the Accountability Agent, where possible." As such, the JOP assessed TRUSTe's application against this standard. Since TRUSTe has indicated that where possible, it will respond to requests from enforcement authorities in APEC economies that reasonably relate to the CBPR-related activities of TRUSTe the JOP is satisfied that TRUSTe meets Recognition Criterion 15.

Case Notes and Statistics

In its application for recognition, TRUSTe requested that it be permitted to fulfill the case note and statistics requirement by drawing "from all TRUSTe-certified companies and not be limited to those companies that have received CBPR certification." While TRUSTe intends to offer CBPR certification under a unique seal, the JOP has confirmed that the certification and monitoring process used by TRUSTe to administer their "Trusted Privacy Seal" is the same as that provided under the CBPR seal.

As stated in Annex D of the *Accountability Agent Application for APEC Recognition*, the objective of the provision of selected case notes is to:

- promote understanding about the operation of the CBPR program;
- assist consumers and businesses and their advisers;
- facilitate consistency in the interpretation of the APEC information privacy principles and the common elements of the CBPR program;
- increase transparency in the CBPR program; and
- promote accountability of those involved in complaints handling and build stakeholder trust in accountability agents.

Annex D further states that “[t]he major objective of the complaints system is to resolve consumer disputes. Subject to the requirements of any particular scheme, this is often facilitated by confidential conciliation or mediation between the parties which does not require, and may even be hampered by, naming respondents publicly.” In consideration of the desirability (or in some instances requirement) to preserve anonymity pursuant to a dispute resolution, the JOP has recommended that Member Economies allow for case notes to be drawn from a wider pool of certified companies, with the provision that all elements required in Annex D be met and that the elements of certification scheme from which those case notes are drawn map to those of the CBPR system.

The JOP has recommended that Member Economies allow for complaint statistics to be drawn from a wider pool of certified companies, again, with the provision that all elements required in Annex E be met and that the elements of the certification scheme from which those case notes are drawn map to those of the CBPR system. The intention behind this recommendation is to facilitate the provision of the broadest data set in order to meet the identified objectives of the complaint statistics reporting requirement.

The JOP recognizes that considerations of anonymization and breadth of data sets behind this recommendation may not apply as an APEC-recognized Accountability Agent’s pool of CBPR-certified companies expands. Should Member Economies determine that the issues raised pursuant to this recommendation require additional specific guidance on the transition from to CBPR-specific case notes and statistics, they should be incorporated into the Accountability Agent Recognition Criteria (Annexes D and E), pursuant to the established endorsement process (the consensus determination of Member Economies).

Finally, the JOP confirms that all case notes and complaint statistics provided by any APEC recognized Accountability Agent will be made publically available through the APEC website and by general email distribution.

Annex A

Program Requirement	Issue Raised	Additional Information
<p>2. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you provide notice that such information is being collected?</p>	<p><i>“TRUSTe only requires a privacy policy to be available. There is no notice requirement for any other circumstances (e.g. application forms, collection over phone etc.)”</i></p>	<p>TRUSTe’s program requirements state that the privacy policy must be present <u>when information is collected</u>. (III.D.5)</p>
<p>3. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you indicate the purpose(s) for which personal information is being collected?</p>	<p><i>“Not a TRUSTe program requirement”</i></p>	<p>TRUSTe’s notice requirements around use cover both first and third parties and do not distinguish between first and third parties. Further third-party disclosure is still required.</p>
<p>7. Do you collect personal information (whether directly or through the use of third parties acting on your behalf) by lawful and fair means, consistent with the requirements of the jurisdiction that governs the collection of such personal information? Where YES, describe.</p>	<p><i>“TRUSTe only requires activities to be lawful and not misleading. There is no test of fairness.”</i></p>	<p>Section 5 of the FTC Act, 15 U.S.C. § 45 gives the Federal Trade Commission (FTC) broad authority to take action against unfair <u>and</u> deceptive acts and practices. As noted in TRUSTe’s Master Services Agreement “Participant represents that it understands that it has an independent duty to comply with any and <u>all</u> laws and regulations.” As such, fairness is a component of lawfulness in this instance.</p>

Program Requirement	Issue Raised	Additional Information
<p>8. Do you limit the use of the personal information you collect (whether directly or through the use of third parties acting on your behalf) as identified in your privacy statement and/or in the notice provided at the time of collection, to those purposes for which the information was collected or for other compatible or related purposes? If necessary, provide a description in the space below.</p>	<p><i>“The TRUSTe program requirement says that use is limited to any purpose ‘reasonably useful’ for the purpose stated at the time of collection. It is unclear what this test means in practice, but it is obviously different from the APEC core principle and should be subject to further analysis.”</i></p>	<p>TRUSTe’s Program Requirement III.C.2a limits <u>use</u> of personal information to “ the provision of those services advertised or provided for, and in accordance with their posted Privacy Statement in effect at the time of collection, or with notice and consent as described in these Program Requirements.” Program requirement III. C.1 further limits <u>collection</u> “to information reasonably useful for the purpose for which it was collected and in accordance with the Participant’s Privacy Statement in effect at the time of collection.”</p>
<p>22. Do you have a mechanism for correcting inaccurate, incomplete and out-dated personal information to the extent necessary for purposes of use?</p>	<p><i>“TRUSTe limits this requirement to ‘commercially reasonable steps’. There is no discussion or analysis of this limitation.”</i></p>	<p>Reasonableness as a standard is found throughout the CBPR Program Requirements. Access and correction includes three qualifications, including “disproportionate burden.” This qualification states that “[p]ersonal information controllers do not need to provide access and correction where the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual’s privacy in the case in question, as for example when claims for access are repetitious or vexatious by nature.” Given the program requirements themselves provide no further analysis of reasonability, the JOP has no endorsed basis upon which to assess TRUSTe’s references to “reasonableness” as it relates to the program requirements under integrity (see TRUSTE program requirements III.E.3.a and III.C.5.a, b).</p>

Program Requirement	Issue Raised	Additional Information
23. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the transfer of the information, do you communicate the corrections to personal information processors, agents, or other service providers to whom the personal information was transferred?	<i>“Not a TRUSTe program requirement”</i>	The obligation of the participant also obligates the service provider in section III.E.5.a.1 – 2. As such, the participant’s obligation to maintain accurate data includes an obligation to ensure third parties, specifically service providers, have accurate data in the first instance.
25. Do you require personal information processors, agents, or other service providers acting on your behalf to inform you when they become aware of information that is inaccurate, incomplete, or out-of-date?	<i>“Not a TRUSTe program requirement”</i>	Section III.E.A of TRUSTe’s program requirements requires steps by the participant to ensure data received from third parties is accurate and requires any third party to report incorrect data to the participant such that the participant is then able to conform to the requirements in this section.
29. Describe how you make your employees aware of the importance of maintaining the security of personal information (e.g. through regular training and oversight).	<i>“Not a TRUSTe program requirement”</i>	The JOP has confirmed that TRUSTe interprets “reasonable security measures” to include the requirement of staff engagement and training.
30. Have you implemented safeguards that are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information...	<i>“The TRUSTe test is proportional to ‘size of the business’ and ‘sensitivity of the data’. This appears to be a completely different test.”</i>	The JOP has confirmed with TRUSTe that a determination of the sensitivity of the information incorporates consideration of the severity of the harm.

Program Requirement	Issue Raised	Additional Information
<p>35. Do you require personal information processors, agents, contractors, or other service providers to whom you transfer personal information to protect against loss, or unauthorized access, destruction, use, modification or disclosure or other misuses of the information by:....b) Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of the personal information of the Applicant's customers?</p>	<p><i>"Not a TRUSTe program requirement"</i></p>	<p>TRUSTe requires the participant to provide data breach notification and to impose equivalent obligations on its third party service providers. As such, third-party service providers must provide notice to the participant for any data breach.</p>
<p>37.a) Do you take steps to confirm the identity of the individual requesting access?</p>	<p><i>"Not a TRUSTe program requirement"</i></p>	<p>TRUSTe access program requirements are related to an "individual." The JOP has confirmed that TRUSTe defines this as the actual data subject. Disclosure of personal information to anyone beyond the data subject would violate TRUSTe's program requirements for both first party and third-party disclosures. Thus, ID verification is required when allowing the "individual" access and correction rights.</p>
<p>37.b) Do you provide access within a reasonable time frame following an individual's request for access?</p>	<p><i>"TRUSTe allows initial period (30 days) to be extended indefinitely. No test of 'reasonable time'"</i></p>	<p>TRUSTe program requirements IV.A.1.a-b require that the provision of access beyond the default 30day period be limited to the timeline established in the participant's privacy statement. The program requirements provide no explicit basis upon which to assess "reasonableness" as it relates to this program requirement. Absent specific guidance, the JOP has determined in its opinion that a default 30 day timeline limited to pre-defined exceptions (to be assessed in advance by TRUSTe) meets this standard.</p>
<p>38.c) Do you make such corrections or deletions within a reasonable time frame following an individual's request for correction or deletion?</p>	<p><i>"Not a TRUSTe program requirement"</i></p>	<p>US law presumes a "commercially reasonableness" standard on all activities which do not have otherwise specified timeframe's associated with them. Since the TRUSTe program requirements offer a right of correction, they must be within a reasonable time under US law.</p>

Program Requirement	Issue Raised	Additional Information
38.e) If access or correction is refused, do you provide the individual with an explanation of why access or correction will not be provided, together with contact information for further inquiries about the denial of access or correction?	<i>“Not a TRUSTe program requirement”</i>	TRUSTe program requirement III.C.5(h) states that “If Participant denies access to PII, Participant must provide the Individual with an explanation of why access was denied and contact information for further inquiries regarding the denial of access.”
39. What measures do you take to ensure compliance with the APEC Information Privacy Principles?	<i>“Not a TRUSTe program requirement”</i>	In the opinion of the JOP, TRUSTe program requirement III.E.1.a.1 (“Participant shall implement controls and processes to manage and protect PII within its control including the ones listed in this III.E”) meets the requirement that a participant ensures compliance with its privacy program requirements.
40. Have you appointed an individual(s) to be responsible for your overall compliance with the Privacy Principles?	<i>“TRUSTe program limits this section to measures ‘Appropriate to the size of the Participant’s business’ – this cannot be right (possibly a mistake in completing the form).”</i>	The JOP has confirmed that TRUSTe’s <i>Master License and Service Agreement Program Amendment – Privacy Program</i> requires the granting of authority by the participant to a named individual to manage the obligations of the privacy certification. In addition, the <i>Master Services Agreement</i> section 11(f) creates a Designated Participant Coordinator responsible for all matters related to any TRUSTe certification, including but not limited to the unique CBPR web seal to be administered by TRUSTe.
42. Do you have procedures in place to ensure individuals receive a timely response to their complaints?	<i>“Not a TRUSTe program requirement (although the master agreement does require the maintenance of a central email contact point)”</i>	The applicable TRUSTe requirement (III.E.6.a) mandates such procedures be “reasonable, appropriate, simple and effective.” The JOP is satisfied that this standard encompasses timeliness.
43. If YES, does this response include an explanation of remedial action relating to their complaint?	<i>“Not a TRUSTe program requirement for its participants”</i>	The JOP has confirmed with TRUSTe that Program Requirement III.E.6.a includes an explanation of any subsequent remedial action taken.

Program Requirement	Issue Raised	Additional Information
44. Do you have procedures in place for training employees with respect to your privacy policies and procedures, including how to respond to privacy-related complaints?	<i>“Not a TRUSTe program requirement”</i>	The JOP has confirmed that TRUSTe interprets “reasonable security measures” under III.E.2a-b.1-4 to include the requirement of staff engagement and training.
47. Do these agreements generally require that personal information processors, agents, contractors or other service providers: ...Impose restrictions on subcontracting unless with your consent?	<i>“Not a TRUSTe program requirement”</i>	The JOP has confirmed that TRUSTe requires that the obligations a participant imposes on third parties apply to any sub-subcontractors in the same manner under II.E.5.a.1-2.
48. Do you require your personal information processors, agents, contractors or other service providers to provide you with self-assessments to ensure compliance with your instructions and/or agreements/contracts? If YES, describe below.	<i>“Not a TRUSTe program requirement”</i>	The JOP has confirmed that III.E.5.a.1-2 requires any participant to take commercially reasonable steps to ensure personal information processors, agents, contractors or other service providers comply with the participants instructions and/or agreements/contracts. As drafted, self- assessments are not a requirement under the CBPR system for such third-parties. However, when used by a participant, the Accountability Agent must verify their existence. Should Member Economies determine that such third-party self-assessments should be made mandatory for CBPR certification, it should be expressly incorporated into the CBPR Program Requirements pursuant to the established endorsement process (the consensus determination of Member Economies).